UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

KENSANDRA SMITH and MARY ELLEN NILLES, Plaintiffs v. LOYOLA UNIVERSITY MEDICAL CENTER, Defendant	No. 23 CV 15828 Judge Jeremy C. Daniel

MEMORANDUM OPINION AND ORDER

Plaintiffs Kensandra Smith and Mary Ellen Nilles filed suit on behalf of themselves and a putative class of similarly situated persons against Loyola University Medical Center ("LUMC"). The plaintiffs allege that LUMC embedded tracking pixels and other devices on its website to collect and transmit personally identifiable health information to third parties like Google and Facebook. (*See generally*, R. 22 ("FAC").)[1] LUMC moves to dismiss the plaintiffs' complaint under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). (R. 32.) For the reasons discussed below, LUMC's motion is granted in part and denied in part.

[1] The Court cites to the sealed version of the plaintiffs' first amended class action complaint. In doing so, the Court is mindful not to reveal information that may be reasonably deemed confidential. To the extent confidential information is discussed, the Court has done so because it is necessary to explain its reasoning. *See In re Specht*, 622 F.3d 697, 701 (7th Cir. 2010) ("Documents that affect the disposition of federal litigation are presumptively open to public view, even if the litigants strongly prefer secrecy, unless a statute, rule, or privilege justifies confidentiality.").

BACKGROUND[2]

Defendant LUMC is a healthcare system consisting of hospitals, primary and specialty care locations, and clinics throughout Chicago, Illinois, and the surrounding area. (FAC ¶¶ 3, 44.)[3] LUMC provides digital healthcare services via an online platform through which current and prospective patients can search for providers, schedule appointments and procedures, communicate with their healthcare providers, review their medical histories, and communicate other information related to their treatment and status as a patient. (*Id.* ¶¶ 44–45.)

The plaintiffs and putative class members are individuals who use LUMC's online platform. (*Id.* ¶¶ 5, 38–39.) They allege that LUMC disclosed their personally identifiable information ("PII") and protected health information ("PHI") to third parties, like Meta Platforms, Inc. d/b/a Meta ("Facebook") and Google LLC d/b/a Google ("Google"), via tracking pixels, first-party cookies, and conversion application programming interface ("CAPI") tools. (*Id.* ¶¶ 3–4, 11, 47.) LUMC configured and installed these tracking tools to bolster its profits by way of targeted advertisements that are created based on the private health information that the plaintiffs inputted on its website. (*Id.* ¶¶ 15, 30.)

[2] The background information is taken from the well-pleaded allegations in the complaint and is accepted as true for purposes of the motion to dismiss. *Demkovich v. St. Andrew the Apostle Par., Calumet City*, 3 F.4th 968, 973 n.2 (7th Cir. 2021).

[3] For CM/ECF filings, the Court cites to the page number(s) set forth in the document's CM/ECF header unless citing to a particular paragraph or other page designation is more appropriate.

LUMC's tracking devices operate as follows: when an individual accesses a certain page on LUMC's website, such as by clicking the "Find a Doctor" tab, the individual's browser sends a request to LUMC's server to load the particular webpage. (*Id.* ¶ 111.) At the same time, the tracking pixels embedded on LUMC's website duplicate the communication and send it to third-party servers, like Facebook, alongside a transcription of the communication's content and the individual's identity. (*Id.*) LUMC's tracking pixels are configured to collect web users' sensitive health information, such as their status as patients, medical appointments, healthcare providers, medical conditions, and treatments. (*Id.* ¶¶ 50, 116–18.) This sensitive health information is then disclosed to companies, like Facebook and Google, alongside web users' IP addresses and "unique Facebook IDs" which, in turn, is used to build marketing and other data profiles to identify, target, and market specific products and services to these individuals. (*Id.* ¶¶ 7, 17, 111, 113–15.)

The named plaintiffs' interactions with LUMC's online platform illustrate this process. Plaintiff Smith alleges that she scheduled a surgical appointment through LUMC's online platform while simultaneously logged into her Facebook account. (*Id.* ¶¶ 123–24.) Shortly thereafter, she began receiving targeted medical advertising related to said surgery on her social media accounts. (*Id.* ¶ 129.) Relatedly, Plaintiff Nilles asserts that, while logged into Facebook, she researched providers who treat certain medical conditions, communicated with said providers, scheduled appointments for said conditions, and reviewed her personal health information, including test results and prescriptions, on LUMC's online platform. (*Id.* ¶¶ 132–33.)

She, too, began receiving targeted advertisements related to her medical conditions and prescriptions on social media. (*Id.* ¶ 138.)

The plaintiffs filed suit on behalf of themselves and two putative classes—a nationwide class and an Illinois class—whose private information was disclosed to third parties through the tracking pixels and related tracking technologies employed on LUMC's online platform. (*Id.* ¶¶ 232–34.) The first amended class action complaint raises a federal claim under the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(1), *et seq.* (Count I), as well as state law claims for negligence (Count II), invasion of privacy (Count III), breach of implied contract (Count IV), unjust enrichment (Count V), breach of implied duty of confidentiality (Count VI), violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"), 815 ILCS 505/1, *et seq.* (Count VII), and violations of the Illinois Eavesdropping Statute, 720 ILCS 5/14, *et seq.* (Count VIII).[4] (*See generally,* FAC.) LUMC moves to dismiss the plaintiffs' first amended class action complaint for lack of standing under Rule 12(b)(1) and for the failure to state a claim under Rule 12(b)(6). (R. 32.)

LEGAL STANDARD

A motion to dismiss under Rule 12(b)(1) challenges the Court's subject matter jurisdiction. *Choice v. Kohn Law Firms, S.C.*, 77 F.4th 636, 638–39 (7th Cir. 2023). Standing is a threshold jurisdictional requirement that "derives from the Constitution's limit on federal courts' authority to resolve 'cases' and 'controversies.'" *Bazile v. Fin. Sys. of Green Bay, Inc.*, 983 F.3d 274, 278 (7th Cir. 2020) (citing U.S.

[4] The Court has subject matter jurisdiction over the plaintiffs' claims under the Class Action Fairness Act, 28 U.S.C. § 1332(d).

Const. art. III, § 2, cl. 1). For facial challenges to standing, the Court accepts all material factual allegations as true and construes all reasonable inferences in the plaintiff's favor. *Id.* at 279. If, however, the defendant challenges standing on factual grounds, the Court may consider and weigh evidence outside the pleadings to determine whether it has jurisdiction over the action. *Id.*

A Rule 12(b)(6) motion, on the other hand, tests whether the plaintiff has provided "enough factual information to state a claim to relief that is plausible on its face" and has raised "a right to relief above the speculative level." *Haywood v. Massage Envy Franchising, LLC*, 887 F.3d 329, 333 (7th Cir. 2018) (citing *Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 736 (7th Cir. 2014)). In deciding a Rule 12(b)(6) motion, the Court accepts as true all well-pleaded factual allegations and draws all reasonable inferences in favor of the non-moving party. *Lax v. Mayorkas*, 20 F.4th 1178, 1181 (7th Cir. 2021). Dismissal is proper where "the allegations . . ., however true, could not raise a claim of entitlement to relief." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 558 (2007).

ANALYSIS

Before addressing LUMC's arguments in support of dismissal, the Court notes that the plaintiffs withdrew several of their common law claims in their response brief, including their claims for invasion of privacy, breach of implied contract, and breach of implied duty of confidentiality. (R. 39 at 4 n.5.) These claims are therefore withdrawn, and the Court will not address them further. *Swiatek v. CVS Pharm., Inc.*, 23 C 1523, 2024 WL 1328801, at *2 (N.D. Ill. Mar. 28, 2024) (addressing only

the plaintiff's non-withdrawn claims on defendant's motion to dismiss); *Jones v. UrbanStrong, LLC*, No. 23 C 3445, 2024 WL 774907, at *1 (N.D. Ill. Feb. 26, 2024) (same); *Wright v. Shumate*, No. 23 C 4734, 2024 WL 689990, at *1 n.4 (N.D. Ill. Feb. 20, 2024) (same).

That leaves the plaintiffs' statutory claims under the ECPA, the ICFA, and the Illinois Eavesdropping Statute, as well as their common law claims for negligence and unjust enrichment. For these claims, the plaintiffs seek declaratory and injunctive relief, in addition to damages. (FAC ¶¶ 289, 306, 388, 410). LUMC argues that none of these claims can proceed, either for lack of standing or for the failure to state a claim.

I. Rule 12(b)(1): Standing

"Because standing is an essential ingredient of subject-matter jurisdiction," the Court begins there. *Bazile*, 983 F.3d at 278. As the party invoking the Court's jurisdiction, the plaintiffs bear the burden of establishing the elements of standing. *Id.* at 278. Those elements are: (1) an injury-in-fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992)). "[A]t the pleading stage, the plaintiff must clearly . . . allege facts demonstrating each element[,]" *id.*, though the facts "need only 'plausibly suggest' each element of standing, with the court drawing all reasonable inferences in the plaintiff's favor." *Bazile*, 983 F.3d at 278 (quoting *Silha v. ACT, Inc.*, 807 F.3d 169, 173–74 (7th Cir. 2015)). In the case of putative class

actions, the named plaintiffs must demonstrate "that they personally have been injured, not that injury has been suffered by other, unidentified members of the class." *Warth v. Seldin*, 422 U.S. 490, 502 (1975).

Here, LUMC makes a facial attack to standing; it argues that the plaintiffs' allegations are insufficient to establish injury-in-fact and traceability. (R. 33 at 4–5.) LUMC contends that the plaintiffs cannot establish either of these elements because they fail to allege with specificity "any actual Sensitive Information (associated with them) allegedly transmitted by using the LUMC website." (*Id.* at 4–5.)

Starting with Article III's injury-in-fact requirement, the harm alleged must be concrete; that is, the injury must be real, not abstract. *See Spokeo*, 578 U.S. at 340. "Both tangible and intangible harms may fit the bill, even if tangible harms like 'physical or monetary injur[ies]' are perhaps intuitively more concrete." *Dinerstein v. Google, LLC*, 73 F.4th 502, 511 (7th Cir. 2023) (quoting *TransUnion*, 594 U.S. at 425). When an intangible harm is asserted, the Court's task is to assess "whether the alleged injury has 'a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts.'" *Id.* (quoting *TransUnion*, 594 U.S. at 425). Congress' views may also be "instructive" when determining whether a harm is sufficiently concrete, and courts "must afford due respect to [Congress'] decision to impose a statutory prohibition . . . on a defendant." *Id.* (citing *Spokeo*, 578 U.S. at 340–41.) Even so, a plaintiff will not automatically satisfy the injury-in-fact requirement simply because "a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." *Spokeo*, 578 U.S. at 341. "Only

those plaintiffs who have been *concretely harmed* by a defendant's statutory violation may sue that private defendant over that violation in federal court." *TransUnion LLC*, 594 U.S. at 427 (emphasis in original).

If a plaintiff alleges that the concrete harm has already materialized, then the plaintiff has standing to seek monetary damages. *See TransUnion*, 594 U.S. at 435–36; *see also Pierre v. Midland Credit Mgt., Inc.*, 29 F.4th 934, 938 (7th Cir. 2022), *cert. denied,* 143 S. Ct. 775 (2023). "[A] risk of future harm is concrete only if the suit is for injunctive relief." *Ewing v. MED-1 Sols., LLC*, 24 F.4th 1146, 1151 (citing *TransUnion*, 494 U.S. 435–36).

Here, the plaintiffs have adequately pleaded injury-in-fact based on the alleged disclosure of their medical information that, at this stage, is sufficient to confer standing to seek both damages and injunctive relief. The alleged disclosure of the plaintiffs' sensitive health information "has a close relationship to disclosure of private information, a common-law theory of harm." *Florence v. Order Express, Inc.*, 674 F. Supp. 3d 472, 479 (N.D. Ill. 2023) (citing *TransUnion*, 594 U.S. at 425); *see also Roper v. Rise Interactive Media & Analytics, LLC* ("*Roper I*")*,* No. 23 C 1836, 2023 WL 7410641, at *3 (N.D. Ill. Nov. 9, 2023) ("Loss of privacy through the disclosure of private information is an intangible harm, but one that courts routinely recognize as concrete" given its close relationship to a traditionally recognized harm).

At common law, the disclosure of private information imposes liability where the defendant gives publicity to a private matter that would be highly offensive to a reasonable person and is not of legitimate concern to the public. *Florence*, 674 F.

Supp. 3d at 480. "[F]acts regarding a person's . . . medical life are inherently private," *Thakkar v. Ocwen Loan Servicing, LLC*, No. 15 C 10109, 2019 WL 2161544, at *13 (N.D. Ill. May 17, 2019) (emphasis omitted), the unauthorized dissemination of which would be "no doubt" highly offensive to a reasonable person. *Roper I*, 2023 WL 7410641, at *4. Nor can it be said that an individual's medical history or diagnoses is generally a matter of legitimate public concern. *Id.*

LUMC does not so much contest the privacy right at issue; rather, it argues that the plaintiffs' allegations of injury are too vague to confer standing. (R. 33 at 4–5.) The first amended complaint, however, alleges in sufficient detail: (1) the types of tracking pixels and other devices installed on LUMC's website; (2) the information that these pixels are designed to capture, including web users' personally identifiable information and private health data; and (3) how this information is intercepted, duplicated, and redirected to third parties like Facebook and Google for marketing purposes. (FAC ¶¶ 72, 75–77, 86–88, 90, 98–100.) Indeed, the named plaintiffs included the specific medical diagnoses and treatment they inputted on LUMC's website, as well as the types of targeted medical advertisements they began receiving shortly thereafter. (*Id.* ¶¶ 129, 133, 138.) Such allegations are sufficient, at this early stage in litigation, for the Court to conclude that the plaintiffs' allegations sufficiently resemble the type of loss protected by the tort of public disclosure of private information such that the loss constitutes an injury-in-fact. *See, e.g., Roper I*, 2023 WL 7410641, at *4 (concluding plaintiffs adequately alleged an injury-in-fact based on unauthorized disclosure of medical diagnoses and health insurance information).

LUMC also argues that the plaintiffs have failed to allege that their injury is "fairly traceable" to any wrongful conduct by LUMC. But Smith and Nilles allege they received unwanted medical advertisements shortly after visiting LUMC's website and inputting their personal medical information. (FAC ¶¶ 129, 138.) Given the close temporal proximity, "[i]t is certainly plausible for pleading purposes that [the plaintiffs'] injuries are 'fairly traceable'" to LUMC's online platform. *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 696 (7th Cir. 2015). Further, both the alleged disclosure of the plaintiffs' medical information, as well as the risk of future harm from subsequent disclosures, is redressable by this Court. The third element of standing is, therefore, also satisfied.

Accordingly, at this stage, the Court concludes that the plaintiffs have established standing to pursue their claims for damages and injunctive relief. Nevertheless, the "standing inquiry remains open to review at all stages of the litigation," and the plaintiffs' burden to show standing will grow heavier as this litigation moves forward. *Persinger v. S.W. Credit Sys., L.P.*, 20 F.4th 1184, 1189 (7th Cir. 2021). LUMC's motion to dismiss the first amended complaint under Rule 12(b)(1) is denied.

II. RULE 12(B)(6): FAILURE TO STATE A CLAIM

LUMC next challenges the plaintiffs' first amended class action complaint on the grounds that the allegations are insufficient to state claims upon which relief may be granted. The Court addresses each of these claims in turn.

a. The Electronic Communications Privacy Act

In Count I, the plaintiffs allege violations of the ECPA. The ECPA provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic communication." 18 U.S.C. § 2511(1)(a). The same is true for those who intentionally disclose or use the contents of an intercepted communication. 18 U.S.C. §§ 2511(1)(c) & (d). Under the so-called "party exception," the ECPA is not violated if the person intercepting the communication "is a party to the communication or where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). The party exception does not apply, however, if the "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." *Id.*

LUMC argues that the plaintiffs' allegations that the tracking pixels operate by duplicating and redirecting their private health data to third parties is insufficient to plausibly allege an unlawful interception because the ECPA requires that the information be "direct[ly]" intercepted during the information's transmission. (R. 33 at 6–7.) The ECPA defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Several circuits have held that the ECPA proscribes only contemporaneous interceptions—that is, an interception that occurs during the transmission of the communication—rather than the acquisition of stored electronic communications, which is addressed under the

Stored Communications Act. *Epstein v. Epstein*, 843 F.3d 1147, 1149–50 (7th Cir. 2016) (collecting cases).

The Seventh Circuit has not taken a position on whether the ECPA covers only contemporaneous interceptions. *Id.* at 1150; *see also United States v. Szymuszkiewicz*, 622 F.3d 701, 705–06 (7th Cir. 2010). Even so, the Seventh Circuit has rejected arguments, such as the one advanced here, that "contemporaneous" means the interception must be "direct." *See Szymuszkiewicz*, 622 F.3d at 705–06 (explaining that "contemporaneous" does not mean that the email communication had to be intercepted "in flight" to violate the Act.) The fact that the plaintiffs allege that the tracking pixels operate by contemporaneously duplicating and redirecting their communications with LUMC's webpage is, therefore, not fatal to their ECPA claim. *See Szymuszkiewicz*, 622 F.3d at 703–04 (holding unlawful interception occurred where email communications were copied at the server and redirected to the defendant within seconds of the original); *see also In re Grp. Health Plan Litig.*, __ F. Supp. 3d __, No. 23 C 267, 2023 WL 8850243, at *6 (D. Minn. Dec. 21, 2023) (finding allegations that defendant "contemporaneously and intentionally" redirected and disclosed plaintiffs' electronic communications to third parties were sufficient to plausibly assert an unlawful interception occurred for purposes of the ECPA).

LUMC further argues that the plaintiffs' allegations are insufficient to show that the "contents" of their communications were disclosed because metadata, such as the URLs from the plaintiffs' browsing history, is not the type of content covered under the Act. (R. 33 at 8–9.) The ECPA broadly defines "contents" to include "any

information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). Courts have explained that, for purposes of the ECPA, "contents" means the "intended message conveyed by the communication." *See Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1076 (N.D. Cal. 2023) (citing *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014)). It does not include "record information regarding the characteristics of the message that is generated in the course of the communication[,]" however. *Id.* (citing *In re Zynga Priv. Litig.*, 750 F.3d at 1106); *see also In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 136 (3d Cir. 2015).

With respect to metadata like URLs, courts have differentiated between those that provide "basic identification and address information," and those that disclose a "search term or similar communication made by the user." *See Meta Platforms, Inc.*, 690 F. Supp. 3d at 1075 (citing *In re Zynga Priv. Litig.*, 750 F.3d at 1108–09). Such courts have reasoned that while the former constitutes record information, the latter qualifies as "content" for purposes of the ECPA. *See id.*; *see also In re Google Inc.*, 806 F.3d at 137 ("URLs may be dialing, routing, addressing, or signaling information, but only when they are performing such a function." If instead a URL is "part of the substantive information conveyed to the recipient, then by definition it is 'content.'"). In this case, the URLs identified in the first amended class action complaint include search terms for specific medical conditions and medical providers. (FAC ¶¶ 125, 135.) This is sufficient to plausibly allege that covered "content" was intercepted. *See,*

e.g., In re Grp. Health Plan Litig., 2023 WL 8850243, at *7; *Meta Platforms, Inc.*, 690 F. Supp. 3d at 1076–77.

Finally, LUMC argues that the plaintiffs' ECPA claim fails under the statute's party exception because LUMC was a party to the communications and consented to the alleged interception "by affirmatively deploying Facebook and Google's website technologies on its website." (R. 33 at 7.) The plaintiffs, in response, rely on the ECPA's crime-tort exception to the party exception. (R. 39 at 10–13.) They allege that LUMC intercepted their electronic communication for the purpose of violating 42 U.S.C. § 1320d-6 of the Health Insurance Portability and Accountability Act ("HIPAA"), and, therefore, LUMC cannot evade liability as a party to the communications under the ECPA. (*Id.* at 11.)

Section 1320d-6 of HIPAA imposes federal criminal liability for one who knowingly disclose "individually identifiable health information" ("IIHI") to third parties. IIHI is any information that:

> (A) is created or received by a health care provider . . . and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and – (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individuals.

42 U.S.C. § 1320(d)(6).

Here, the plaintiffs allege that LUMC, via the tracking devices employed on its webpages, transmitted the plaintiffs' status as medical patients, the content of their communications with LUMC's webpage, information about their medical

appointments, location of treatments, specific medical providers, specific medical conditions and treatments, and other sensitive health information to third parties. (FAC ¶ 50.) While the plaintiffs make this allegation "[u]pon information and good faith belief," (*id.*), the Court notes that they do not have direct access to what goes on in the background of LUMC's online platforms to be able to provide further details to support their claims of improper disclosures of personal health information. *See, e.g., Kurowski v. Rush Sys. for Health* (*Kurowski III*), No. 22 C 5380, 2023 WL 8544084, at *3 (N.D. Ill. Dec. 11, 2023) (acknowledging the plaintiffs' lack of behind-the-scenes knowledge regarding the defendant, Facebook, and Google's web properties in evaluating the sufficiency of their allegations).

Lacking the benefit of discovery, Smith and Nilles' allegations regarding their individual experiences using LUMC's online platform—and the inferences drawn from those experiences—are sufficient to plausibly allege that LUMC disclosed information regarding their personal health conditions and treatments to third parties. (FAC ¶¶ 129, 133, 138.) Such information qualifies as IIHI for purposes of HIPAA. Further, the plaintiffs allege that LUMC's collection and disclosure of their personal health information was done knowingly and for purposes of financial gain—namely, to bolster profits via targeted marketing campaigns. (*Id.* ¶¶ 15, 193–97, 271, 276.) Taken as a whole, these allegations are sufficient to invoke HIPPA for purposes of the ECPA's crime-tort exception. *See, e.g., Kurowski III*, 2023 WL 8544084, at *3. Accordingly, LUMC's motion to dismiss Count I is denied.

b. Negligence

In Count II, the plaintiffs assert a claim for common law negligence. To state a claim for negligence under Illinois law, "a plaintiff must plead that the defendant owed a duty of care to the plaintiff, that the defendant breached that duty, and that the breach was the proximate cause of the plaintiff's injuries." *Cowper v. Nyberg*, 28 N.E.3d 768, 772 (Ill. 2015) (citing *Mt. Zion State Bank & Tr. v. Consol. Commc'ns, Inc.*, 660 N.E.2d 863, 867–68 (Ill. 1995)).

LUMC first argues that the plaintiffs have failed to plausibly allege that it owed them a duty to prevent the disclosure of their private health information. (R. 33 at 9.) In support of this argument, LUMC relies on *Cooney v. Chicago Public Schools*, 943 N.E.2d 23 (Ill. App. Ct. 2010), which declined to recognize a new common law duty to safeguard personal information. *Id.* at 28–29 ("While we do not minimize the importance of protecting this information, we do not believe that the creation of a new legal duty beyond legislative requirements already in place is part of our role on appellate review."). As this Court and other courts have discussed, however, the Illinois legislature has since created a duty that requires data collectors "to maintain reasonable security measures under the Information Protection Act." *Flores v. Aon Corp.*, __ N.E.3d __, 2023 IL App (1st) 230140, ¶ 23 (Ill. App. Ct. 2023) (citing *In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 590 (N.D. Ill. 2022)); *see also In re Mondelez Data Breach Litig.,* No. 23 C 3999, 2024 WL 2817489, at *4 (N.D. Ill. June 3, 2024); *Wittmeyer v. Heartland All. For Hum. Needs & Rts.*, No. 23 C 1108, 2024 WL 183311, at *2 (N.D. Ill. Jan. 17, 2024); 815 ILCS 530/45.

LUMC nonetheless argues that the reasoning of *Cooney* still applies in cases that do not involve allegations of a data breach. (R. 33 at 9 n.3.) The Court is not persuaded by this logic. Illinois' Personal Information Protection Act ("PIPA") requires data collectors, *i.e.*, entities that handle, collect, disseminate, or otherwise deal with nonpublic personal information, to protect this information from "unauthorized access, acquisition, destruction, use, modification, or disclosure." 815 ILCS 530/45(a); *see also* 815 ILCS 530/5. The complaint alleges that LUMC collected the plaintiffs' nonpublic personal information and disseminated that information to unauthorized third parties. Thus, the complaint plausibly alleges a duty to prevent the disclosure of their private health information.

Next, LUMC argues that the plaintiffs' negligence claim fails because they have not plausibly alleged compensable damages. (R. 33 at 9–10.) Illinois law requires a plaintiff to plead "a legally cognizable present injury or damage to sustain a negligence claim." *Leslie v. Medline Indus., Inc.*, No. 20 C 1654, 2021 WL 4477923, at *7 (N.D. Ill. Sept. 30, 2021) (citing *Yu v. Int'l Bus. Machs. Corp.*, 732 N.E.2d 1173, 1177 (Ill. App. Ct. 2000)). Here, the plaintiffs allege that they have suffered "fear, anxiety and worry" about the status of, and the loss of control over, their private health information. (FAC ¶ 304.) Allegations of emotional harm, such as these, are sufficient to state a negligence claim under Illinois law, including in the data privacy context. *See, e.g., Roper v. Rise Interactive Media & Analytics, LLC* ("*Roper II*"), No. 23 C 1836, 2024 WL 1556298, at *2 (N.D. Ill. Apr. 10, 2024) (citing *In re Gallagher*,

631 F. Supp. 3d 573 at 587). Because these facts, if proven, could satisfy the present injury requirement, LUMC's motion to dismiss Count II is denied.[5]

c. Illinois Consumer Fraud and Deceptive Business Practices Act

In Count VII, the plaintiffs allege that LUMC engaged in unfair acts and practices in violation of the ICFA. "In order to state a claim under the ICFA, a plaintiff must show: '(1) a deceptive or unfair act or promise by the defendant; (2) the defendant's intent that the plaintiff rely on the deceptive or unfair practice; and (3) that the unfair or deceptive practice occurred during a course of conduct involving trade or commerce.'" *Camasta*, 761 F.3d at 739 (quoting *Wigod v. Wells Fargo Bank, N.A.*, 673 F.3d 547, 574 (7th Cir. 2012)). The plaintiff must also "plausibly plead that the deceptive or unfair act caused her to suffer actual damages, meaning pecuniary loss." *Benson v. Fannie May Confections Brands, Inc.*, 944 F.3d 639, 647 (7th Cir. 2019) (citing *Kim v. Carter's Inc.*, 598 F.3d 362, 365 (7th Cir. 2010)).

LUMC argues that the plaintiffs' ICFA claim cannot proceed because (1) the plaintiffs are not "consumers" within the meaning of the statute, (2) they cannot plausibly allege that the defendant's conduct was deceptive or unfair, (3) they have not pleaded actual, pecuniary loss, and (4) they cannot invoke PIPA as a basis for

[5] LUMC appears to suggest that Illinois' economic loss doctrine precludes the plaintiffs' negligence claim as well. (R. 33 at 9.) But the economic loss doctrine, also known as the *Moorman* doctrine, bars tort recovery for purely economic losses based on the failure to perform contractual obligations. *Catalan v. GMAC Mortg. Corp.*, 629 F.3d 676, 692–93 (7th Cir. 2011) (citing *Moorman v. Mfg. Co. v. Nat'l Tank Co.*, 435 N.E.2d 443, 448–49 (Ill. 1982)). The plaintiffs do not allege that an express contractual obligation governed LUMC's duty to safeguard their health data. The economic loss doctrine is therefore inapplicable. *See, e.g., Wittmeyer,* 2024 WL 182211, at *3.

their ICFA claim. (R. 33 at 18–22.) Because the plaintiffs have failed to allege the specific economic damages necessary to bring their claim under the ICFA, the Court begins and ends its analysis there.

The ICFA provides remedies for "purely economic injuries." *Flores*, 2023 IL App (1st) 230140, ¶ 41 (citing *Morris v. Harvey Cycle & Camper, Inc.*, 911 N.E.2d 1049, 1053 (Ill. App. Ct. 2009)). "Actual damages must be calculable and 'measured by the [plaintiffs'] loss.'" *Morris*, 911 N.E.2d at 1053 (quoting *Chicago v. Mich. Beach Hous. Coop.*, 696 N.E.2d 804, 811 (Ill. App. Ct. 1998)). "The failure to allege specific economic damages precludes a claim brought under the [ICFA]." *Flores*, 2023 IL App (1st) 230140, ¶ 41.

The plaintiffs allege that they suffered actual monetary loss in the form of "overpaying" for LUMC's health services. (R. 39 at 20–21.) They say that they purchased healthcare services from LUMC and utilized its online platform based on the defendant's representation that their personal health information would be protected and not disclosed to unauthorized third parties. (*Id.* at 20.) But for this representation, the plaintiffs "would not have used [LUMC's] services or would have paid less for those services." (FAC ¶ 343.)

This type of "benefit of the bargain" theory of damages, however, has been repeatedly rejected for non-products liability claims such as this. *See Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 968 (7th Cir. 2016) (citing *Remijas*, 794 F.3d at 695) (explaining that benefit of the bargain theories "have been adopted by courts only where the product itself was defective or dangerous and consumers claim they

would not have bought it (or paid a premium for it) had they known of the defect"); *cf. In re Aqua Dots Prods. Liab. Litig.*, 654 F.3d 748, 751 (7th Cir. 2011) (acknowledging financial injury when plaintiffs "paid more for the toys than they would have, had they known of the risks the bads posed to children"). The plaintiffs do not cite any authority that would otherwise support a benefit of the bargain theory in the context of data privacy. *Cf. Kurowski v. Rush System for Health* (*"Kurowski II"*), 683 F. Supp. 3d 836, 846 (N.D. Ill. 2023) (declining to expand the benefit of the bargain theory to plaintiffs' ICFA claim based on the defendant's failure to protect private health information).

Accordingly, the plaintiffs' benefit of the bargain theory does not plausibly allege a monetary loss for purposes of the ICFA. Nor can the plaintiffs rely on their allegation that LUMC's conduct caused a diminution in value of their personal data to allege an actionable harm for purposes of the ICFA. (FAC ¶ 229); *see, e.g., Flores*, 2023 IL App (1st) 230140, ¶ 42 (declining to hold that "diminution in the value of personal information is a specific economic injury under the [ICFA]"). LUMC's motion to dismiss Count VII is therefore granted.

d. Unjust Enrichment

In Count V, the plaintiffs plead a claim for unjust enrichment. Unjust enrichment, however, "is not a separate cause of action under Illinois law." *Horist v. Sudler & Co.*, 941 F.3d 274, 281 (7th Cir. 2019); *see also Benson*, 944 F.3d at 648 (citing *All. Acceptance Co. v. Yale Ins. Agency, Inc.*, 648 N.E.2d 971, 977 (Ill. App. Ct. 1975), relying on *Charles Hester Enters., Inc. v. Ill. Founders Ins. Co.*, 484 N.E.2d 349,

354 (Ill. App. Ct. 1985), *aff'd*, 499 N.E.2d 1319 (1986)). "[I]f an unjust enrichment claim rests on the same improper conduct alleged in another claim, then the unjust enrichment claim will be tied to this related claim—and, of course, unjust enrichment will stand or fall with the related claim." *Cleary v. Philip Morris Inc.*, 656 F.3d 511, 517 (7th Cir. 2011); *see also Flores*, 2023 IL App (1st) 230140, ¶ 37.

Like their ICFA claim, the plaintiffs' unjust enrichment claim alleges that LUMC collected, used, and disclosed the plaintiffs' personal health data for its own financial gain under the guise that such information would be kept private. (FAC ¶¶ 342–43.) Because that is the same improper conduct alleged in their ICFA claim, the plaintiffs' unjust enrichment claim cannot stand. *See, e.g., Ramirez v. LexisNexis Risk Sols.,* __ F. Supp. 3d __, No. 22 C 5384, 2024 WL 1521448, at *8 (N.D. Ill. Apr. 8, 2024). LUMC's motion to dismiss Count V is therefore granted.

e. Illinois Eavesdropping Statute

In Count VIII, the plaintiffs allege violations of the Illinois Eavesdropping Statute. This statute creates a civil cause of action against an eavesdropper who knowingly, intentionally, and surreptitiously "[u]ses an eavesdropping device" to transmit or record "all or any part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation." 720 ILCS 5/14-2(a)(2); *see also* 720 ILCS 5/14-6 (civil remedies). The definition of "eavesdropping device" includes any device capable of being used to intercept or transcribe electronic communications. 720 ILCS 5/14-1(a). The statute also prohibits the use or disclosure of any information which the eavesdropper "knows

or reasonably should know was obtained from a private conversation or private electronic communication. . . unless he or she does so with the consent of all of the parties." 720 ILCS 5/14-2(a)(5).

LUMC first invokes its "interception" challenge that it raised with respect to the plaintiffs' ECPA claim as reason to dismiss their eavesdropping claim. (R. 33 at 22.) But the Court rejected that argument, and does so here, too.

Next, LUMC contends that the plaintiffs cannot plausibly state a claim under the Illinois Eavesdropping Statute because the statute only applies to a person who is not a party to the communication. (R. 33 at 22–23.) LUMC is correct that the statute proscribes use of an eavesdropping device by a non-party for the purpose of "overhearing, transmitting, or recording all or any part of any private conversation," 720 ILCS 5/14-2(a), but that is only one way in which the statute may be violated. Here, the plaintiffs allege violations based on use of an eavesdropping device "for the purpose of transmitting or recording all or any part of any private conversation to which he or she *is a party*." (FAC ¶ 390 (citing 720 ILCS 5/14-2(a)(2)). That LUMC is alleged to have been a party to the intercepted communications is, thus, not fatal to the plaintiffs' claim.

Finally, LUMC asserts that the plaintiffs' eavesdropping claim fails because LUMC discloses on its website that it automatically collects certain information from its web users and therefore any interception was not surreptitious. (R. 33 at 23.) But the disclosure on LUMC's website is limited in scope. It applies only to categories of information like a web user's "IP address, browser type, computer or device type, the

website from where you navigated to our Site and the pages on our Site that you view." (FAC ¶ 106.) The disclosure does not inform web users that their personal health information will be collected and disclosed to third parties. Rather, LUMC's Notice of Privacy Practices provides that the defendant "will only use or disclose [protected health information] as permitted or required by applicable state law." (*Id.* ¶ 101.) Notwithstanding this notice, the plaintiffs allege that LUMC collected their personal health information via tracking pixels and disclosed this information to third parties without their knowledge, authorization, or consent. (*Id.* ¶¶ 127, 136.) The Court finds that such allegations are sufficient to plausibly allege "surreptitious" conduct for purposes of the Illinois Eavesdropping Statute. *See* 720 ILCS 5/14-1(g) ("'[S]urreptitious' means obtained or made by stealth or deception, or executed through secrecy or concealment."). LUMC's motion to dismiss Count VIII is denied.

f. Preemption

Finally, LUMC contends that the plaintiffs' common law claims are preempted by PIPA. (R. 33 at 23–25.) Preemption is an affirmative defense upon which the defendants bear the burden of proof. *See Benson*, 944 F.3d at 645; *Treadwell v. Power Sols. Int'l, Inc.*, 427 F. Supp. 3d 984, 989 (N.D. Ill. 2019) (citing *Baylay v. Etihad Airways P.J.S.C.*, 881 F.3d 1032, 1039 (7th Cir. 2018)). Affirmative defenses do not generally justify dismissal under Rule 12(b)(6). *Doe v. GTE Corp.*, 347 F.3d 655, 657 (7th Cir. 2003). This is because a plaintiff "need not anticipate and attempt to plead around defenses" in the complaint. *Chi. Bldg. Design, P.C. v. Mongolian House, Inc.*, 770 F.3d 610, 613–14 (7th Cir. 2014). Dismissal based on an affirmative defense is

appropriate only in the limited circumstances where "the allegations of the complaint itself set forth everything necessary to satisfy the affirmative defense." *Id.* at 614 (citing *United States v. Lewis*, 411 F.3d 838, 842 (7th Cir. 2005)).

Here, the only remaining common law cause of action is the plaintiffs' negligence claim. Because PIPA does not expressly abrogate any existing common-law remedy, LUMC's argument that the statute preempts the plaintiffs' negligence claim "rests on the proposition that preemption was accomplished by implication." *Callahan v. Edgewater Care & Rehab. Ctr., Inc.*, 872 N.E.2d 551, 570 (Ill. App. Ct. 2007). "Repeal or preemption of an existing common-law remedy by implication is not favored." *Id.* at 570–71 (citing *Shores v. Senior Manor Nursing Ctr., Inc.*, 518 N.E.2d 471, 475 (Ill. App. Ct. 1988)). "The rule has long been that a statute will not be construed as taking away a common-law right existing at the time of its enactment unless the pre-existing right is so repugnant to the statute that the survival of the common-law right would in effect deprive the statute of its efficacy and render its provisions nugatory." *Id.* at 571.

Based on this standard, the Court does not find that the plaintiffs have pleaded themselves out of court on the basis of preemption, particularly when Illinois courts have allowed common law claims, like negligence, to proceed in the data privacy context notwithstanding PIPA. *See, e.g., Flores*, 2023 IL App (1st) 230140, ¶ 25. Accordingly, the Court denies LUMC's motion to dismiss based on the affirmative defense of preemption.

CONCLUSION

Defendant Loyola University Medical Center's motion to dismiss [32] is granted in part and denied in part. LUMC's motion to dismiss the plaintiffs' first amended class action complaint under Federal Rule of Civil Procedure 12(b)(1) is denied, as is LUMC's motion to dismiss Counts I, II, and VIII under Federal Rule of Civil Procedure 12(b)(6). The Court grants, under Rule 12(b)(6), LUMC's motion to dismiss Counts V and VII. The Court, consistent with the plaintiffs' withdrawal of these claims, dismisses Counts III, IV, and VI. The plaintiffs are granted leave to amend their ICFA and unjust enrichment claims (Counts V and VII) if they can do so consistent with this Memorandum Opinion and Rule 11 of the Federal Rules of Civil Procedure. *See* Fed. R. Civ. P. 15(a)(2); *Runnion ex rel. Runnion v. Girl Scouts of Greater Chi. and N.W. Ind.*, 786 F.3d 510, 519 (7th Cir. 2015). The plaintiffs shall file a proposed amended complaint, if they so choose to do so, on or before July 23, 2024.

Date: July 9, 2024

JEREMY C. DANIEL
United States District Judge